

IN THE CLAIMS:

1. (Currently Amended) A security gateway for securely connecting a plurality of networks; comprising:

a logical interface to a first network;

a logical interface to a second network;

a physical interface to a third network that is an untrusted network;

a logical interface to a fourth network, via said third network, that is a protected resource network;

a processor configured to execute packet handling rules for:

denying at least some client access through the gateway from a host in the untrusted network to hosts in the first network, in the second network and in the protected resource network;

denying at least some client access through the gateway from a host in the second network to a host in the first network; and

permitting at least some client access through the gateway from a host in the first network to hosts in the second network and in the protected resource network.

1 2. (Original) The security gateway of claim 1, wherein the processor is further
2 configured to execute packet handling rules for translating a source network address in a
3 packet sent to the second network.

1 3. (Original) The security gateway of claim 2, wherein the packet handling rules for
2 translating translate the source network address of a packet sent to the second network to
3 be the network address of the security gateway interface to the second network.

1 4. (Original) The security gateway of claim 1, wherein the processor is further
2 configured to execute packet handling rules for permitting at least some client access
3 through the gateway from a host in the first network to a host in the untrusted network.

1 5. (Original) The security gateway of claim 4, wherein the processor is further
2 configured to execute packet handling rules for translating a source network address in a
3 packet sent to the untrusted network.

1 6. (Original) The security gateway of claim 5, wherein the packet handling rules for
2 translating translate the source network address of a packet sent to the untrusted network
3 to be the network address of the security gateway interface to the untrusted network.

1 7. (Original) The security gateway of claim 1, wherein the processor is further
2 configured to execute packet handling rules for permitting at least some client access
3 through the gateway from a host in the protected resource network to a host in the first
4 network.

1 8. (Original) The security gateway of claim 1, wherein the processor is further
2 configured to execute packet handling rules for denying at least some client access
3 through the gateway from a host in the protected resource network to a host in the first
4 network.

1 9. (Original) The security gateway of claim 1, wherein the processor is further
2 configured to execute packet handling rules for permitting at least some client access
3 through the gateway from a host in the second network to a host in the untrusted network.

1 10. (Original) The security gateway of claim 9, wherein the processor is further
2 configured to execute packet handling rules for translating a source network address in a
3 packet sent to the untrusted network.

1 11. (Original) The security gateway of claim 10, wherein the packet handling rules
2 for translating translate the source network address of a packet sent to the untrusted
3 network to be the network address of the security gateway interface to the untrusted
4 network.

1 12. (Original) The security gateway of claim 1, further comprising a protected
2 network service, and the processor is further configured to execute packet handling rules

3 for denying at least some access from at least one network to the protected network
4 service.

1 13. (Original) The security gateway of claim 12, wherein the protected network
2 service is a mail relay.

1 14. (Original) The security gateway of claim 1, wherein the interface to the protected
2 resource network includes a VPN tunnel utilizing the untrusted network.

1 15. (Original) The security gateway of claim 1, wherein the processor is further
2 configured to execute packet handling rules for denying at least some client access
3 through the gateway from a host in the protected resource network to a host in the second
4 network.

1 16. (Original) The security gateway of claim 1, wherein the processor is further
2 configured to execute packet handling rules for denying at least some client access
3 through the gateway from a host in the protected resource network to a host in the
4 untrusted network.

1 17. (Original) The security gateway of claim 1, wherein the processor is further
2 configured to execute packet handling rules for denying at least some client access
3 through the gateway from a host in the second network to a host in the protected resource
4 network.

1 18. (Original) The security gateway of claim 1, wherein the logical interface to the
2 first network is a logical interface to a first trust-group network, and the logical interface
3 to the second network is a logical interface to a second trust-group network.

1 19. (Original) The security gateway of claim 1, wherein the logical interface to the
2 first network is a logical interface to a first local network, and the logical interface to the
3 second network is a logical interface to a second local network.

1 20. (Original) The security gateway of claim 1, wherein the logical interface to the
2 protected resource network is a logical interface to a remote corporate network.

1 21. (Original) The security gateway of claim 1, wherein the processor is further
2 configured to execute packet handling rules for:
3 denying at least some client access through the gateway from a
4 host in the second network to a host in the protected resource network; and
5 denying at least some client access through the gateway from a
6 host in the protected resource network to hosts in the second network and
7 in the untrusted network.

1 22. (Original) The security gateway of claim 21, wherein the interface to the
2 protected resource network includes a VPN tunnel utilizing the untrusted network.

1 23. (Original) The security gateway of claim 22, wherein the processor is further
2 configured to execute packet handling rules for permitting at least some client access
3 through the gateway from a host in the second network to a host in the untrusted network.

1 24. (Original) The security gateway of claim 23, wherein the processor is further
2 configured to execute packet handling rules for permitting at least some client access
3 through the gateway from a host in the first network to a host in the untrusted network.

1 25. (Currently Amended) A machine readable medium containing configuration
2 instructions for performing a method for securely connecting a plurality of networks
3 through a security gateway having a logical interface to a first network, a logical interface
4 to a second network, a physical interface to a third network that is an untrusted network
5 and a logical interface to a fourth network that is a protected resource network where said
6 logical interface to said fourth network is via said third network, the method comprising
7 the steps of:

8 denying at least some client access through the gateway from a host in the
9 untrusted network to hosts in the first network, in the second network and in the protected
10 resource network;

11 denying at least some client access through the gateway from a host in the
12 second network to a host in the first network; and

13 permitting at least some client access through the gateway from a host in
14 the first network to hosts in the second network and in the protected resource network.

1 26. (Original) The machine readable medium of claim 25, wherein the method
2 further comprises the step of translating a source network address in a packet sent to the
3 second local network.

1 27. (Original) The machine readable medium of claim 26, wherein the translating
2 step includes translating the source network address of a packet sent to the second
3 network to be the network address of the security gateway interface to the second
4 network.

1 28. (Original) The machine readable medium of claim 25, wherein the method
2 further comprises the step of permitting at least some client access through the gateway
3 from a host in the first network to a host in the untrusted network.

1 29. (Original) The machine readable medium of claim 28, wherein the method
2 further comprises the step of translating a source network address in a packet sent to the
3 untrusted network.

1 30. (Original) The machine readable medium of claim 29, wherein the translating
2 step includes translating the source network address of a packets sent to the untrusted
3 network to be the network address of the security gateway interface to the untrusted
4 network.

1 31. (Original) The machine readable medium of claim 25, wherein the method
2 further comprises the step of permitting at least some client access through the gateway
3 from a host in the protected resource network to a host in the first network.

1 32. (Original) The machine readable medium of claim 25, wherein the method
2 further comprises the step of denying at least some client access through the gateway
3 from a host in the protected resource network to a host in the first network.

1 33. (Original) The machine readable medium of claim 25, wherein the method
2 further comprises the step of permitting at least some client access through the gateway
3 from a host in the second network to a host in the untrusted network.

1 34. (Original) The machine readable medium of claim 33, wherein the method
2 further comprises the step of translating a source network address in a packet sent to the
3 untrusted network.

1 35. (Original) The machine readable medium of claim 34, wherein the translating
2 step includes translating the source network address of a packet sent to the untrusted
3 network to be the network address of the security gateway interface to the untrusted
4 network.

1 36. (Original) The machine readable medium of claim 25, wherein the security
2 gateway further has a protected network service, and the method further comprises the
3 step of denying at least some access from at least one network to the protected network
4 service.

1 37. (Original) The machine readable medium of claim 36, wherein the protected
2 network service is a mail relay.

1 38. (Original) The machine readable medium of claim 25, wherein the interface to
2 the protected resource network includes a VPN tunnel utilizing the untrusted network.

1 39. (Original) The machine readable medium of claim 25, wherein the method
2 further comprises the step of denying at least some client access through the gateway
3 from a host in the protected resource network to a host in the second network.

1 40. (Original) The machine readable medium of claim 25, wherein the method
2 further comprises the step of denying at least some client access through the gateway
3 from a host in the protected resource network to a host in the untrusted network.

1 41. (Original) The machine readable medium of claim 25, wherein the method
2 further comprises the step of denying at least some client access through the gateway
3 from a host in the second network to a host in the protected resource network.

1 42. (Currently Amended) A method for securely connecting a plurality of networks
2 through a security gateway having a logical interface to a first network, a logical interface
3 to a second network, a physical interface to a third network that is an untrusted network
4 and a logical interface to a fourth network that is a protected resource network, said
5 logical interface to said fourth network being via said third network; the method
6 comprising the steps of:
7 denying at least some client access through the gateway from a host in the
8 untrusted network to hosts in the first network, in the second network and in the protected
9 resource network;
10 denying client access from a host in the second network to a host in the
11 first network; and
12 permitting client access from a host in the first network to hosts in the
13 second network and in the protected resource network.

1 43. (Original) The method of claim 42, further comprising the step of translating a
2 source network address in a packet sent to the second network.

1 44. (Original) The method of claim 43, wherein the translating step includes
2 translating the source network address of a packet sent to the second network to be the
3 network address of the security gateway interface to the second network.

1 45. (Original) The method of claim 42, further comprising the step of permitting at
2 least some client access through the gateway from a host in the first network to a host in
3 the untrusted network.

1 46. (Original) The method of claim 45, further comprising the step of translating a
2 source network address in a packet sent to the untrusted network.

1 47. (Original) The method of claim 46, wherein the translating step includes
2 translating the source network address of a packet sent to the untrusted network to be the
3 network address of the security gateway interface to the untrusted network.

1 48. (Original) The method of claim 42, further comprising the step of permitting at
2 least some client access through the gateway from a host in the protected resource
3 network to a host in the first network.

1 49. (Original) The method of claim 42, further comprising the step of denying at
2 least some client access through the gateway from a host in the protected resource
3 network to a host in the first network.

1 50. (Original) The method of claim 42, further comprising the step of permitting at
2 least some client access through the gateway from a host in the second network to a host
3 in the untrusted network.

1 51. (Original) The method of claim 50, further comprising the step of translating a
2 source network address in a packet sent to the untrusted network.

1 52. (Original) The method of claim 51, wherein the translating step includes
2 translating the source network address of a packet sent to the untrusted network to be the
3 network address of the security gateway interface to the untrusted network.

1 53. (Original) The method of claim 52, wherein the security gateway further has a
2 protected network service, and the method further comprises the step of denying at least
3 some access from at least one network to the protected network service.

1 54. (Original) The method of claim 53, wherein the protected network service is a
2 mail relay.

1 55. (Original) The method of claim 42, wherein the interface to the protected
2 resource network includes a VPN tunnel utilizing the untrusted network.

1 56. (Original) The method of claim 42, further comprising the step of denying at
2 least some client access through the gateway from a host in the protected resource
3 network to a host in the second network.

1 57. (Original) The method of claim 42, further comprising the step of denying at
2 least some client access through the gateway from a host in the protected resource
3 network to a host in the untrusted network.

1 58. (Original) The method of claim 42, further comprising the step of denying at
2 least some client access through the gateway from a host in the second network to a host
3 in the protected resource network.